REMARKS

The present application was filed on February 19, 2004, with claims 1-33, and claims priority to U.S. provisional application Serial No. 60/468,200, filed May 6, 2003. Claims 1-33 are currently pending in the application. Claims 1 and 30-33 are the independent claims.

Reconsideration of the present application is respectfully requested in view of the following remarks.

Claims 1, 2, 4-8, 20, 23-25, 30, 32 and 33 stand rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,842,106 (hereinafter "Hughes") in view of U.S. Patent No. 4,928,098 (hereinafter "Dannhaeuser").

Claims 3, 9-16, 26-29 and 31 stand rejected under §103(a) over Hughes and Dannhaeuser in combination with other references.

Claims 17-19, 21 and 22 are indicated as containing allowable subject matter.

Applicant initially notes with regard to claim 31, that the Examiner at page 4, last line, of the final Office Action, states that claim 31 "recites the combination of claims 1 and 3." Also, on page 10, second paragraph, the Examiner characterizes claim 31 as reciting "a system for practicing the combination of method claims 1 and 3." These characterizations of claim 31 are clearly incorrect. For example, claim 3 specifies that "transmitted pseudonyms are authenticated by a verifier other than the reader." This limitation is not present in claim 31. Also, claim 31 recites a plurality of RFID devices and a plurality of readers, while claim 1 recites at least one RFID device and at least one reader. Accordingly, the above-noted characterizations regarding claim 31 are improper and should be withdrawn.

With regard to the §103(a) rejection of claims 1, 2, 4-8, 20, 23-25, 30, 32 and 33 over Hughes and Dannhaeuser, Applicant respectfully traverses.

A proper *prima facie* case of obviousness requires that the combination of references must teach or suggest all the claim limitations, and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine or modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicant submits that the Examiner has failed to establish a proper *prima facie* case of obviousness in the §103(a) rejection of independent claim 1, in that the collective disclosures of Hughes and Dannhaeuser fail to teach or suggest all the claim limitations, and in that no cogent

motivation has been identified for combining or modifying the reference teachings to reach the claimed invention.

Independent claim 1 is directed to a method for use in an RFID system comprising at least one RFID device and at least one reader which communicates with the RFID device. The method includes the steps of associating a plurality of pseudonyms with the RFID device, and transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device. The claim further specifies that an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

Applicant notes that an RFID device, by its very nature, necessarily transmits device-identifying information. See the specification at, for example, page 1, line 19, to page 2, line 15, and page 4, line 28, to page 5, line 26.

It is also important to note that claim 1 requires the association of a plurality of pseudonyms with an RFID device, with different ones of the pseudonyms being transmitted by the device in response to different reader queries of the RFID device. A given reader query of an RFID device constitutes a request for the device-identifying information of that device, as is apparent from, for example, page 5, lines 24-26, of the specification.

In the invention of claim 1, an authorized verifier, which may be a reader, is able to determine that the different transmitted pseudonyms are associated with the same RFID device. This advantageously results in an arrangement in which the RFID device can be authenticated without the need for complex cryptographic operations, thereby overcoming a significant problem of the prior art. See the specification at, for example, page 2, lines 12-25, and page 4, lines 11-15.

The Examiner argues that the proposed combination of Hughes and Dannhaeuser teaches each and every limitation of claim 1. Applicant respectfully disagrees. In formulating the rejection, the Examiner argues that the secret key value 66 stored in memory 50 of each tag 44 in Hughes constitutes one or more pseudonyms as claimed. See the final Office Action at page 6, last paragraph. However, the secret key value 66 cannot reasonably be construed as comprising a plurality of pseudonyms, or even a single pseudonym. As noted above, a pseudonym as that term is used in the present specification and in standard usage implies some ability to identify a particular entity with which the pseudonym is associated. In the Hughes system, the same secret

key value 66 is stored in each of the tags 44, as indicated at column 5, lines 47-50. Thus, the secret key value itself does not provide any device-identifying information whatsoever, and accordingly is not a pseudonym for the device. Instead, Hughes teaches to use a conventional identification code to identify a particular tag to the reader. See Hughes at, for example, column 5, lines 7-8 and 21-23. The tags in the Hughes system are therefore configured to "broadcast their identifiers in a promiscuous manner to any nearby readers." See the specification at page 2, lines 12-15. Hughes addresses this problem through the use of a complex challenge-response authentication process, of the type referred to at page 2, lines 16-22, of the specification, rather than through the use of pseudonyms as claimed. Thus, Hughes is believed to teach away from the claimed arrangements.

In addition, the Hughes approach suffers from exactly the same problem identified by Applicant at page 2, lines 12-22, of the specification, in that it requires an unduly complex cryptographic arrangement in order to provide authentication. As indicated previously, the claimed arrangements advantageously overcome this problem.

Moreover, Applicant notes that the secret key value 66 is apparently not transmitted by any of the RFID tags in Hughes. As noted above, claim 1 calls for the transmission of different pseudonyms of an RFID device in response to different reader queries of that device. The Examiner argues that the secret key value 66 meets the claimed pseudonym, but such a value is not transmitted by its corresponding device, as would be required by explicit recitations in claim 1. The pseudorandom values that are processed using the secret key value 66 and transmitted as part of the Hughes challenge-response authentication process do not constitute pseudonyms as claimed, again because such pseudorandom values do not provide any device-identifying information. Thus, Hughes appears to teach directly away from the present invention, and suffers from the same problem that is advantageously addressed and solved by the claimed arrangements.

The Examiner acknowledges that Hughes alone fails to meet the limitations of claim 1, but argues that the deficiencies of Hughes are overcome by Dannhaeuser. However, the automobile remote keyless entry codes in Dannhaeuser do not constitute pseudonyms as claimed, because the codes do not provide any ability to uniquely identify a particular code transmitting device. In the remote keyless entry context of the Dannhaeuser system, it is well known that for a given automobile, the owner is typically provided with multiple redundant remote keyless entry

devices. The codes shown in the table in column 3 of Dannhaeuser would therefore have to be replicated on each such device. As a result, the codes themselves cannot be used to uniquely identify any particular one of the multiple devices. The Dannhaeuser codes are therefore not pseudonyms as recited in the claim. Moreover, because the Dannhaeuser devices do not transmit device-identifying information, those devices are not RFID devices as claimed.

It should be pointed out in this regard that remote keyless entry devices would not be understood by one skilled in the art to constitute RFID devices of the type recited in the claim at issue. Remote keyless entry devices simply transmit a code which if found to match a code in a corresponding receiver causes the receiver to perform some action, such as unlocking a car. RFID devices, on the other hand, emit device-identifying information in response to a reader query, thereby allowing the reader to uniquely identify the particular device with which it is communicating. Thus, it is believed that RFID devices and remote keyless entry devices are entirely different types of devices, and one looking to improve RFID device would generally not look to the remote keyless entry device art. The Dannhaeuser teachings are therefore believed to represent non-analogous art relative to the Hughes reference.

Accordingly, it is believed that the collective teachings of Hughes and Dannhaeuser therefore fail to meet the pseudonym transmission aspects of claim 1.

Inasmuch as claim 1 includes limitations not taught or suggested by the combined teachings of Hughes and Dannhaeuser, the Examiner has failed to establish a *prima facie* case of obviousness for this claim.

Also, as indicated previously, the Examiner has failed to identify a cogent motivation for combining the Hughes and Dannhaeuser references or for modifying their teachings to reach the claimed invention. The claimed arrangement advantageously overcomes the above-noted problems associated with the conventional approach of configuring RFID tags to "broadcast their identifiers in a promiscuous manner to any nearby readers." Hughes, by teaching use of such an identifier broadcasting approach in conjunction with challenge-response authentication, directly teaches away from the claimed invention, and fails to provide its associated advantages. Similarly, Dannhaeuser teaches to transmit remote keyless entry codes, which may be replicated on multiple devices and hence do not uniquely identify any particular device. Accordingly, there is no objective evidence of record which would lead one skilled in the art to combine or modify Hughes and Dannhaeuser to reach the claimed invention.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344. As noted above, there has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine or modify the Hughes and Dannhaeuser references to produce the particular limitations in question.

Instead of objective evidence of motivation to combine or modify Hughes and Dannhaeuser, the Examiner simply provides conclusory statements. For example, the Examiner states that it would be obvious to combine Hughes and Dannhaeuser "because it provides security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses." See the final Office Action at page 7, second paragraph.

The Examiner apparently argues that it would be obvious to apply the remote keyless entry code rotation process of Dannhaeuser to the secret key value 66 of Hughes to provide improved security. However, such an arrangement would clearly be undesirable in an RFID system having a very large number of tags. Hughes teaches that the same secret key value 66 is stored in each of the tags. In a typical RFID system, there are thousands of such tags. If the Dannhaeuser code rotation were applied to the secret key value 66 of Hughes, it would appear to be very difficult and highly impractical to coordinate such secret key value rotation between all the tags and the reader. The rotation is possible in the Dannhaeuser automobile remote keyless entry context because there are usually only a few remote keyless entry devices per automobile. Moreover, Hughes provides a challenge-response authentication process to address the security issue raised by the Examiner, and thus there is no apparent need in the Hughes system for code rotation of the type disclosed in Dannhaeuser. Accordingly, it is believed that the Dannhaeuser technique is not only undesirable in an RFID system, it is practically unworkable in such a system. It is also contrary to the objectives of the claimed invention in terms of providing

techniques implementable in low-cost RFID devices with limited computational and storage resources.

It therefore appears that the Examiner in formulating the §103(a) rejection of claim 1 over Hughes and Dannhaeuser has undertaken a piecemeal reconstruction of the claimed invention based upon impermissible hindsight, given the benefit of the disclosure provided by Applicant.

Thus, the §103(a) rejection of claim 1 over Hughes and Dannhaeuser is believed to be improper, and should be withdrawn.

Dependent claims 2, 4-8, 20 and 23-25 are believed allowable for at least the reasons identified above with regard to independent claim 1.

Independent claims 30, 31 and 32 include limitations similar to those of independent claim 1, and are therefore believed allowable for reasons similar to those identified above.

Applicant further notes with regard to claim 33 that the Examiner is incorrect in stating at page 9, second to last paragraph, of the final Office Action that claim 33 "recites the limitations of claim 1." Claim 33 does not include the wherein clause of claim 1, and does not refer to an RFID system or RFID devices. See the specification at, for example, page 5, lines 2-7. Claim 33 recites that pseudonyms are determined utilizing an updatable set of one or more one-time pads maintained in a device. The Examiner argues that the claimed updatable set of one or more one-time pads is disclosed by the "index designators" in column 4, lines 5-24, of Dannhaeuser. Applicant respectfully disagrees. As is well known to one skilled in the cryptographic arts, a "one-time pad" is a type of cryptographic construct, an example of which is described in the specification at page 10, lines 11-17. The relied-upon portion of Dannhaeuser makes no reference whatsoever to any aspect of cryptography, much less to one-time pads as claimed.

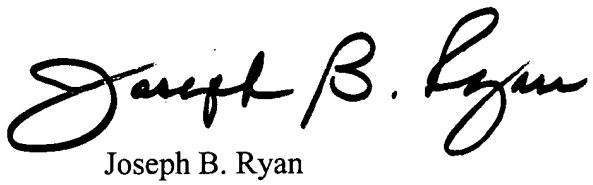
Applicant notes that the foregoing reference to a cryptographic construct cannot reasonably be viewed as arguing a limitation that is not present in the claim. A one-time pad is in fact a cryptographic construct, as indicated in the specification and as is well known to those skilled in this art, and the relied-upon portions of Dannhaeuser do not provide any disclosure regarding one-time pads. As a result, the obviousness rejection of claim 33 based on Hughes and Dannhaeuser is fundamentally flawed and should be withdrawn.

Dependent claims 3, 9-16 and 26-29 are believed allowable for at least the reasons identified above with regard to independent claim 1. The additional cited references fail to overcome the fundamental deficiencies of Hughes and Dannhaeuser as identified above.

Accordingly, claims 1-33 are believed to be in condition for allowance.

As indicated previously, a Notice of Appeal is submitted concurrently herewith.

Respectfully submitted,



Date: November 2, 2005

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Enclosure(s): Notice of Appeal